WHAT IS CLAIMED IS:

1. A data processing system, comprising:

at least one main processor connected to a system bus;

a system memory connected to the system bus and accessible to each of the main processors;

a tamper mechanism configured to change state responsive to insertion of the system into a slot in a rack enclosure; and

means for determining system information including geographical address information and for communicating the information externally.

2. The system of claim 1, wherein the means for determining the geographical address include a local service processor connected to a set of physical identification connector pins indicative of the geographical address of a slot in which the system is inserted.

3. The system of claim 1, wherein the means for communicating externally comprise a communication bus connected to a local service processor of the system.

4. The system of claim 3, wherein the communication bus comprises an RS-485 communication bus to which the local service processor is connected.

5

5. The system of claim 1, wherein, responsive to a power-on event, a local server processor of the system is configured to determine the system's geographical address, the state of its tamper latch, and to communicate the geographical address and tamper latch information externally.

10

6. The system of claim 5, wherein the system is configured, responsive to determining that the tamper latch is in an altered state, to configure a functional boot image on the system.

7. The system of claim 5, wherein, responsive to determining that the tamper latch is in an altered state, the service processor is configured to issue an external alert identifying the system by its geographical address.

8. The system of claim 7, wherein the external alert further identifies the system by system information selected from the list including an identifier of a network interface card of the system, a UUID, and a main processor serial number.

9. A data processing network, comprising:

a management module comprising a management module service processor and a memory; and

a plurality of server blades connected to a common network, each blade comprising a system memory connected to at least one main processor, a tamper mechanism configured to change state responsive to insertion of the corresponding blade into a slot in a rack enclosure, and means for determining a geographical address of the slot occupied by

the blade and for communicating the determined address to the management module.

10. The network of claim 9, wherein the means for determining the geographical address include a local service processor connected to a set of physical identification connector pins indicative of the geographical address of a slot in which the system is inserted.

11. The network of claim 9, wherein the means for communicating externally comprise a communication bus connecting a local service processor of each server blade to the management module.

12. The network of claim 11, wherein the communication bus comprises an RS-485 communication bus to which each local service processor is connected.

13. The network of claim 9, wherein, responsive to a power-on event, a local server processor of each server blade is configured to determine the blade's geographical address, the state of its tamper latch, and to communicate the geographical address and tamper latch information to the management module.

14. The network of claim 13, wherein each server blade is configured, responsive to determining that its tamper latch is in an altered state, to configure a functional boot image on the server blade.

15. The network of claim 13, wherein, responsive to determining that the tamper latch is in an altered state, the service processor is configured to issue an external alert to the management identifying the system by its geographical address.

16. The network of claim 15, wherein the external alert further identifies the system by system information selected from the list including an identifier of a network interface card of the system, a UUID, and a main processor serial number.

17. The network of claim 16, wherein the management module is configured to communicate the system information to a system deployment module.

18. A computer program product comprising a set of computer executable instructions for monitoring system information in a data processing network, the instructions being stored on a computer readable medium, comprising:

computer code means for determining the state of a tamper latch of a data processing system;

computer code means for determining the geographical address of the data processing system;

computer code means for communicating the tamper latch and geographical address information to a management module connected to the data processing system.

19. The computer program product of claim C, wherein the code means for determining the geographical address include code means for a reading a set of physical identification pins of the data processing system, wherein the state of the pins is indicative of the geographical address of a slot in which the system is inserted.

20. The computer program product of claim C, wherein the code means for determining the blade's geographical address, the state of its tamper latch, and communicating the geographical address and tamper latch information to the management module is responsive to a power-on event.

21. The computer program product of claim 20, further comprising code means for configuring a functional boot image on the server blade responsive to determining that the tamper latch is in an altered state.

22. The computer program product of claim 20, further comprising code means for issuing an external alert identifying the system by its geographical address responsive to determining that the tamper latch is in an altered state.

23. The computer program product of claim 22, wherein the external alert further identifies the system by system information selected from the list including an identifier of a network interface card of the system, a UUID, and a main processor serial number.